LISTING OF CLAIMS

This listing will replace all prior versions, and listings, of claims in the application:

1. (Original) In a data communications device, a method providing authentication of a client device to a server device, the method comprising the steps of:

    detecting a requirement for authentication of a request for data sent from a client device to a server device;

    creating an authentication response in response to the step of detecting the requirement for authentication, the authentication response containing authentication information required by the server device to allow the client device to access data via the server device;

    inserting the authentication response into the data communications session between the client device and the server device, the authentication response authenticating, to the server device, access to the data by the client device;

    maintaining the data communications session between the server device and the client device in the presence of authentication response information inserted into the data communications session between the client device and the server device.

2. (Original) The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises the step of:

    detecting, in a data communications session between a client device and a server device, an authentication request sent from the server device to the client device for authentication of the client device by the server device.

3. (Original) The method of claim 2 wherein the step of detecting an authentication request comprises the step of:

    intercepting an unauthorized response sent from the server device to the client device over the data communications session, the unauthorized response indicating that the server device requires authentication of the client device in order for the client device to access the data using the server device.

4. (Original) The method of claim 3 wherein the unauthorized response from the server device is generated by the server device in response to an unauthenticated request for data sent from the client device to the server device over the data communications session.

5. (Original) The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises the steps of:

    detecting, in a data communications session between a client device and a server device, a request for data sent from a client device to a server device for access to data using the server device;

    caching the request for data in the data communications device; and

    detecting, in the data communications session between a client device and a server device, an authentication request sent from the server device to the client device for authentication of the request for data sent from the client device to the server device.

6. (Original) The method of claim 1 wherein the step of creating an authentication response comprises the steps of:

    obtaining authentication information associated with the client device, the authentication information capable of authorizing, on behalf of the client device, access to the data using the server device; and

    incorporating the authentication information into the authentication response such that the authentication response, when received by the server device due to the step of inserting, allows the server device to authenticate access, by the client device, to data using the server device.

7. (Original) The method of claim 6 wherein:

    the authentication information is access control information; and

    wherein the step of incorporating comprises the steps of:

placing the access control information into an authentication header of a packet of data serving as the authentication response to allow the client device to access restricted data using the server device;

adjusting connection information associated with the packet of data to account for the authentication information incorporated into the authentication response; and

formatting the authentication response to appear as though it originated from the client device.

8. (Original) The method of claim 1 wherein:

the authentication response is a packet including an authentication header containing the authentication information and is created by the data communications device to appear as though it originated from the client device; and

wherein the step of inserting the authentication response into the data communications session between the client device and the server device comprises the step of forwarding the authentication response to the server device over the data communication session as at least one packet of extra data, the authentication response being formatted to appear as though it originated from the client device.

9. (Original) The method claim 1 wherein the steps of detecting, creating, inserting and maintaining are performed by the data communications device without assistance from the client device and are performed such that the data communications session between the client device and the server device is free from disruption due to authentication requirements of the client device to the server device.

10. (Original) The method of claim 1 wherein the step of maintaining the data communications session between the server device and the client device after inserting the authentication response into the data communications session comprises the steps of:

maintaining connection state data in the data communications device that tracks an amount of extra data associated with the authentication response that is inserted into the data communications session between the client device and the server device; and

modifying connection information within packets passing through the data communications device that are exchanged between the client device and server device using the data communications session in order to allow the client and server device to maintain proper respective first and second connection states for the data communications session regardless of the amount of extra data added in the data communications session due to insertion of the authentication response.

11. (Currently amended) The method of claim 1 wherein:

the steps of detecting, creating, inserting and maintaining are repeated for at least a first and second iteration; and

wherein for the first iteration:

the step of detecting a requirement for authentication of a request for data comprises the step of detecting an authentication request sent over the data communications session from the server device to the client device in response to the client device providing a first request for access to data using the server device; and

wherein for the first iteration, the step of creating an authentication response comprises the steps of recreating the first request for access to first data and placing authentication information into the recreated first request to allow the server device to authenticate the recreated first request upon ~~begin~~ being received by the server device in the step of inserting.

12. (Original) The method of claim 11 wherein, for the second iteration of the steps of detecting, creating, inserting and maintaining:

the step of detecting a requirement for authentication of a request for data comprises the step of detecting a second request for access to data sent from the client device to the server device; and

wherein for the second iteration, the step of creating an authentication response comprises the steps of:

intercepting the second request for access to data; and

generating an authentication response by inserting the authentication information as an authentication header into the second request to allow the server device to authenticate the second request for data on behalf of the client device without requiring generation of an authentication request; and

wherein for the second iteration, the step of inserting the authentication response into the data communications session between the client device and the server device comprises the step of:

forwarding the second request containing the authentication header to the server device such that the server device can authenticate the second request.

13. (Original) The method of claim 1 wherein the step of detecting a requirement for authentication of a request for data sent from a client device to a server device comprises at least one of the steps of:

a) detecting an authentication request being transmitted from a server device through the data communications device to a client device in response to the client device providing a first request for data to the server device that requires authentication by the server device; and

b) detecting a second request for data being transmitted through the data communications device from the client device to the server device and detecting that the client device provided a first request for data to the same server device.

14. (Original) The method of claim 1 wherein:

the data communications session is a transmission control protocol session between the client device and the server device; and

wherein the step of maintaining modifies connection information within messages exchanged between the client device and the service device to account for the insertion of authentication information inserted into the data communications session in order to

provide automatic authentication of requests for data sent to the server device on behalf of client devices.

15. (Original) The method of claim 1 wherein the steps of detecting, creating, inserting and maintaining are performed on behalf of a plurality of client devices and wherein the authentication information is selected in the step of creating from different sets of authentication information based on at least one of an address of the client device, an address of the server device, a type of data specified in the request, and a protocol used to provide the request.

16. (Original) The method of claim 1 wherein the data communications device is a device operating in a network to which hypertext transport protocol traffic is redirected to perform the steps of detecting, creating, inserting and maintaining.

17. (Original) A data communications device comprising:

at least one communications interface;

a memory;

a processor; and

an interconnection mechanism coupling the at least one communications interface, the memory and the processor;

wherein the memory is encoded with an authentication manager application that when performed on the processor, produces an authentication manager process that causes the data communications device to provide authentication of a client device to a server device by performing the operations of:

detecting a requirement for authentication of a request for data sent from a client device to a server device;

creating an authentication response in response to the step of detecting the requirement for authentication, the authentication response containing authentication information required by the server device to allow the client device to access data via the server device;

inserting the authentication response into the data communications session between the client device and the server device on the at least one communications interface, the authentication response authenticating, to the server device, access to the data by the client device;

maintaining the data communications session between the server device and the client device in the presence of authentication response information inserted into the data communications session between the client device and the server device.

18. (Original) The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform the step of:

detecting, in a data communications session between a client device and a server device passing through the at least one communications interface, an authentication request sent from the server device to the client device for authentication of the client device by the server device.

19. (Original) The data communications device of claim 18 wherein when the authentication manager process causes the data communications device to perform the step of detecting an authentication request, the authentication manager process causes the data communications device to perform the step of:

intercepting, on the at least one communications interface, an unauthorized response sent from the server device to the client device over the data communications session, the unauthorized response indicating that the server device requires authentication of the client device in order for the client device to access the data using the server device.

20. (Original) The data communications device of claim 19 wherein the unauthorized response from the server device is generated by the server device in response to an

unauthenticated request for data sent from the client device to the server device over the data communications session.

21. (Original) The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform the step of:

detecting, in a data communications session between a client device and a server device, a request for data sent from a client device to a server device for access to data using the server device;

caching the request for data in the data communications device; and

detecting, in the data communications session between a client device and a server device, an authentication request sent from the server device to the client device for authentication of the request for data sent from the client device to the server device.

22. (Original) The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of creating an authentication response, the authentication manager process causes the data communications device to perform the step of:

obtaining authentication information associated with the client device, the authentication information capable of authorizing, on behalf of the client device, access to the data using the server device; and

incorporating the authentication information into the authentication response such that the authentication response, when received by the server device due to the step of inserting, allows the server device to authenticate access, by the client device, to data using the server device.

23. (Original) The data communications device of claim 22 wherein:

the authentication information is access control information; and

wherein when the authentication manager process causes the data communications device to perform the step of incorporating, the authentication manager process causes the data communications device to perform the steps of:

placing the access control information into an authentication header of a packet of data serving as the authentication response to allow the client device to access restricted data using the server device;

adjusting connection information associated with the packet of data to account for the authentication information incorporated into the authentication response; and

formatting the authentication response to appear as though it originated from the client device.

24. (Original) The data communications device of claim 17 wherein:

the authentication response is a packet including an authentication header containing the authentication information and is created by the data communications device to appear as though it originated from the client device; and

wherein when the authentication manager process causes the data communications device to perform the step of inserting the authentication response into the data communications session between the client device and the server device, wherein when the authentication manager process causes the data communications device to perform the step of forwarding the authentication response to the server device over the data communication session as at least one packet of extra data, the authentication response being formatted to appear as though it originated from the client device.

25. (Original) The data communications device claim 17 wherein the steps of detecting, creating, inserting and maintaining are performed by the data communications device without assistance from the client device and are performed such that the data communications session between the client device and the server

device is free from disruption due to authentication requirements of the client device to the server device.

26. (Original) The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of maintaining the data communications session between the server device and the client device after inserting the authentication response into the data communications session, the authentication manager process causes the data communications device to perform the steps of:

maintaining connection state data in the data communications device that tracks an amount of extra data associated with the authentication response that is inserted into the data communications session between the client device and the server device; and

modifying connection information within packets passing through the data communications device that are exchanged between the client device and server device using the data communications session in order to allow the client and server device to maintain proper respective first and second connection states for the data communications session regardless of the amount of extra data added in the data communications session due to insertion of the authentication response.

27. (Original) The data communications device of claim 17 wherein:

the authentication manager causes the data communications device to repeat the steps of detecting, creating, inserting and maintaining for at least a first and second iteration; and

wherein for the first iteration:

when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data, the authentication manager process causes the data communications device to perform the step of detecting an authentication request sent over the data communications session from the server device to the client device in response to the client device providing a first request for access to data using the server device; and

wherein for the first iteration, when the authentication manager process causes the data communications device to perform the step of creating an authentication response, the authentication manager process causes the data communications device to perform the steps of recreating the first request for access to first data and placing authentication information into the recreated first request to allow the server device to authenticate the recreated first request upon begin received by the server device in the step of inserting.

28. (Original) The data communications device of claim 27 wherein, for the second iteration of the steps of detecting, creating, inserting and maintaining:

when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data, the authentication manager process causes the data communications device to perform the step of detecting a second request for access to data sent from the client device to the server device; and

wherein for the second iteration, when the authentication manager process causes the data communications device to perform the step of creating an authentication response, the authentication manager process causes the data communications device to perform the steps of:

intercepting the second request for access to data; and

generating an authentication response by inserting the authentication information as an authentication header into the second request to allow the server device to authenticate the second request for data on behalf of the client device without requiring generation of an authentication request; and

wherein for the second iteration, the authentication manager process causes the data communications device to perform the step of inserting the authentication response into the data communications session between the client device and the server device, the authentication manager process causes the data communications device to perform the step of:

forwarding the second request containing the authentication header to the server device such that the server device can authenticate the second request.

29. (Original) The data communications device of claim 17 wherein when the authentication manager process causes the data communications device to perform the step of detecting a requirement for authentication of a request for data sent from a client device to a server device, the authentication manager process causes the data communications device to perform at least one of the steps of:

a) detecting an authentication request being transmitted from a server device through the data communications device to a client device in response to the client device providing a first request for data to the server device that requires authentication by the server device; and

b) detecting a second request for data being transmitted through the data communications device from the client device to the server device and detecting that the client device provided a first request for data to the same server device.

30. (Original) The data communications device of claim 17 wherein:

the data communications session is a transmission control protocol session between the client device and the server device; and

wherein when the authentication manager process causes the data communications device to perform the step of maintaining, the data communications device modifies connection information within messages exchanged between the client device and the service device over the at least one communications interface to account for the insertion of authentication information inserted into the data communications session in order to provide automatic authentication of requests for data sent to the server device on behalf of client devices.

31. (Original) The data communications device of claim 17 wherein the steps of detecting, creating, inserting and maintaining are performed on behalf of a plurality of client devices using the same authentication information, and wherein the authentication information is selected from different sets of authentication information based on at least

one of an address of the client device, an address of the server device, a type of data specified in the request, and a protocol used to provide the request.

32. (Original) The data communications device of claim 17 wherein the data communications device is a device operating in a network to which hypertext transport protocol traffic is redirected to perform the steps of detecting, creating, inserting and maintaining.

33. (Original) A computer program product having a computer-readable medium including computer program logic encoded thereon that, when performed on a computer system having a coupling of a memory, a processor, and at least one communications interface, provides a method for authenticating a client device to a server device by performing the operations of:

    detecting a requirement for authentication of a request for data sent from a client device to a server device;

    creating, on the processor, an authentication response in memory in response to the step of detecting the requirement for authentication, the authentication response containing authentication information required by the server device to allow the client device to access data via the server device;

    inserting the authentication response into the data communications session between the client device and the server device on the at least one communications interface, the authentication response authenticating, to the server device, access to the data by the client device;

    maintaining the data communications session between the server device and the client device in the presence of authentication response information inserted into the data communications session between the client device and the server device.

34. (Original) A data communications device comprising:

    at least one communications interface;

    a memory;

    a processor; and

an interconnection mechanism coupling the at least one communications interface, the memory and the processor;

wherein the memory is encoded with an authentication manager application that when performed on the processor, produces an authentication manager process that causes the data communications device to provide authentication of a client device to a server device by providing a means including:

means for detecting a requirement for authentication of a request for data sent from a client device to a server device;

means for creating an authentication response in response to the step of detecting the requirement for authentication, the authentication response containing authentication information required by the server device to allow the client device to access data via the server device;

means for inserting the authentication response into the data communications session between the client device and the server device on the at least one communications interface, the authentication response authenticating, to the server device, access to the data by the client device;

means for maintaining the data communications session between the server device and the client device in the presence of authentication response information inserted into the data communications session between the client device and the server device.

35. (New) The method of claim 14 wherein:

the data communications session is a single transmission control protocol session between the client device and the server device and utilizes a single application layer protocol; and

wherein the step of maintaining modifies connection information within messages exchanged between the client device and the service device to account for the insertion of authentication information inserted into the data communications session in order to provide automatic authentication of requests for data sent to the server device on behalf of client devices.

36. (New) The data communications device of claim 30 wherein:

the data communications session is a single transmission control protocol session between the client device and the server device and utilizes a single application layer protocol; and

wherein when the authentication manager process causes the data communications device to perform the step of maintaining, the data communications device modifies connection information within messages exchanged between the client device and the service device over the at least one communications interface to account for the insertion of authentication information inserted into the data communications session in order to provide automatic authentication of requests for data sent to the server device on behalf of client devices.